Расширения полей I: Алгебраические числа

Задача 1. Приведите пример ненулевого многочлена с рациональным коэффициентами, корнем которого является а) $1+\sqrt[3]{2}$; б) $\sqrt{2}+\sqrt{3}$; в*) $\sqrt[3]{2}+\sqrt{3}$; г*) $(1+\sqrt[3]{2})\sqrt{3}$.

▷ **Определение 1.** Действительное число называется *алгебраическим*, если оно является корнем ненулевого многочлена с рациональными коэффициентами, и *трансцендентным* в противном случае.

Задача 2*. а) Трансцендентные числа существуют.
б*) Приведите конкретный пример трансцендентного числа.

Задача 3*. Алгебраические числа образуют поле.

▷ **Определение 2.** *Минимальным многочленом* алгебраического числа α называется неприводимый многочлен $m_\alpha \in \mathbb{Q}[x]$, такой что $m_\alpha(\alpha)=0$. *Степенью* алгебраического числа называется степень его минимального многочлена.

Задача 4. а) Любое алгебраическое число степени 2 может быть представлено в виде $a \pm \sqrt{d}$, где числа a и d рациональные. (Верно ли аналогичное утверждение для алгебраических чисел степени 4?)
б) Если $\alpha = a+\sqrt{d}$ (числа a и d рациональные), то $m_\alpha = (x-\alpha)(x-\bar{\alpha})$, где $\bar{\alpha} = a-\sqrt{d}$.

Задача 5. а) $\{P \in \mathbb{Q}[x] : P(\alpha)=0\} = (m_\alpha)$.
б) Минимальный многочлен алгебраического числа α существует и единственен (с точностью до умножения на ненулевую константу).

Задача 6. Если α — алгебраическое действительное число, то внутри действительных чисел есть подполе $\mathbb{Q}(\alpha)$, изоморфное полю $\mathbb{Q}[x]/(m_\alpha)$.

▷ **Определение 3.** Пусть L поле, K его подполе («L/K[1] — расширение полей»). Говорят, что элемент поля L *алгебраичен* над K, если он является корнем ненулевого многочлена с коэффициентами в K. (Таким образом, выше шла речь об алгебраических элементах в расширении $\mathbb{R}/\mathbb{Q}$.)

Расширение L/K называется *алгебраическим*, если любой его элемент алгебраичен.

Задача 7. Любое конечное поле характеристики p является алгебраическим расширением поля $\mathbb{F}_p$.

Задача 8. Любое расширение конечных полей получается последовательностью расширений вида $K \subset L \cong K[x]/(P)$.

Задача 9. Если конечное поле имеет характеристику p, то количество элементов в нем является степенью числа p.

Задача 10. Для любого поля K и любого многочлена P над этим полем найдется расширение, в котором многочлен P а) имеет корень; б) раскладывается на линейные множители.

Задача 11. а) Если L — поле из $q=p^n$ элементов, то любой его элемент является корнем многочлена $x^q - x$.
б) Для любого q вида p^n существует поле из q элементов.
в*) Единственно ли такое поле?

[1] Читается «L над K», не путать с фактором.